IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH/SEIZURE OF:

Black and Gray Samsung Phone, IMEI: 354266114682650

Magistrate No. 3:21-51 MJ

[UNDER SEAL]

AFFIDAVIT

I, Staci M. Johnson, being duly sworn, do hereby state and depose as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a United States Postal Inspector with the United States Postal Inspection Service ("USPIS") and have been so employed since August 2004. I am currently assigned to the Narcotics and Money Laundering Team at the USPIS's Pittsburgh, Pennsylvania field office. In this capacity, I am responsible for investigating the use of the United States Mails for the purpose of transporting controlled substances such as marijuana, methamphetamine, heroin, fentanyl, fentanyl-related analogs, cocaine, and other controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) (manufacturing, distribution, or possession with the intent to manufacture or distribute a controlled substance), 843(b) (unlawful use of a communication facility in the commission of a crime), and 846 (drug conspiracy).

2. This affidavit is made in support of an application for a warrant to search the following electronic device:

1. Black and Gray Samsung Phone, IMEI: 354266114682650

3. This electronic device is associated with Jeffery Sheeder (hereinafter "SHEEDER"). As more fully explained below, SHEEDER is believed to be involved in the distribution of various narcotics, including marijuana, cocaine and LSD in the Western District of

Pennsylvania, primarily, Bedford County. Accordingly, law enforcement has probable cause to believe that a search of this electronic device will produce evidence of violations of federal felony offenses, as enumerated in Title 21, United States Code, Section 846 (drug conspiracy) and Title 21, United States Code, Sections 841(a)(1) (manufacturing, distribution, or possession with the intent to manufacture or distribute a controlled substance).

4. I have reviewed information obtained from law enforcement and commercial databases and discussed this case with and reviewed the reports of other law enforcement officers who have been involved in this investigation. This Affidavit is being submitted for the limited and specific purpose of supporting an application for search and seizure warrants. I have not, therefore, included every fact I know concerning the investigation.

5. As more fully explained below, there is probable cause to conclude that evidence of trafficking of narcotics will be found in the electronic device known to be associated with SHEEDER, which is the subject of this search warrant affidavit (hereafter occasionally referred to as the "Subject Electronic Device"). As a result of my training and experience, I am aware individuals involved in distributing illegal drugs commonly store or retain evidence of their involvement in drug trafficking on their cellular telephones and other electronic devices, including but not limited to: incoming/outgoing call logs, contact lists, text messages, photographs, videos, and voicemails.

STATEMENT OF PROBABLE CAUSE

Narcotics Parcels

6. Your Affiant became aware of 10869 Clear Ridge Road, Everett, PA 15537 receiving suspected narcotics parcels since November 2020. Through search of postal records and databases, several parcels that were delivered to the aforementioned address had return

addresses that were associated with prior seizures of Xanax pills, marijuana and subject of investigations into methamphetamine to other delivery addresses across the country.

On March 25, 2021, your affiant identified suspect Priority Mail parcel 9505 5131 9116 1082 8161 21 addressed to "Jeff sheeder, 10869 Clear ridge rd, Everett, PA 15537," with the return address of Sage Jerichson, 1218 NE 135th ave, Portland, OR 97230." It should be noted that E-bay tape was wrapped around the seams of the parcel.

6. An electronic inquiries of the CLEAR database was made for the purpose of confirming the validity of the recipient's name and address contained on the Subject Parcel. The CLEAR inquiry confirmed 10869 Clear Ridge Road, Everett, PA is a valid address in the 15537 zip code, and the name Jeffrey Sheeder does associate to this address.

7. The CLEAR database was made for the purposes of confirming the validity of the sender's name and address contained on the Subject Parcel. The CLEAR inquiry confirmed 1218 NE 135th Avenue, Portland OR is a valid address in the 97230 zip code, however the name Sage Jerichson does not associate to that address. Furthermore, Sage Jerichson does not associate to any address in the state of Oregon. CLEAR has proven to be reliable in previous investigations in determining the validity of names and addresses.

8. On March 25, 2021, your affiant and Pennsylvania State Trooper Michael McCullough attempted to make contact with the resident of 10869 Clear Ridge Road. While at that time no one answered the door, your affiant observed an empty cardboard box with E-bay tape around the seams bearing tracking number 9505 5131 9118 1074 9508 24. The parcel was addressed to Jeff Sheeder and from "Sage Jerichson, 1218 NE 135th ave, Portland, OR 97230."

9. Your affiant and Trooper McCullough returned later in the day on March 25, 2021 in another attempt to make contact with a resident at 10869 Clear Ridge Road, Everett, PA. At this time a

white male, later identified as Caleb Christian Luzier, answered the door. Your affiant could smell the distinct odor of burnt marijuana when the door was opened. I identified myself and stated I was looking for Jeff Sheeder. Luzier stated Sheeder was at work. Luzier was asked if he had contact information for Sheeder and he stated he could contact him. Luzier placed the call on speaker phone and Sheeder stated he was not expecting a parcel. When Sheeder was informed that the parcel in your affiant's possession had the same sender information and E-bay tape as a box that was on the side of his residence, Sheeder stated the empty parcel was a drill he ordered. Sheeder was asked to return to the residence. Sheeder stated he would need a ride and he consented to be being picked up at his place of work to the residence by law enforcement.

10. While waiting for Sheeder, Luzier was asked if he lived at the residence. Luzier stated he did not live there but was sleeping on Sheeder's couch that night and helping him out by watching his dog. Luzier was informed he could leave if he did not want to stay at the residence. Luzier was told he could take any personal belongings with him, at which time Luzier stated he only had his coat and plastic bag from a convenience store that contained candy. Luzier was asked if he had any other possessions there and he stated he did not even have a change of clothes. Luzier's identification and phone number were obtained and then he left the premises.

11. While waiting for Sheeder, your affiant made contact with the Everett Post Office to ask if personnel was familiar with the aforementioned address. One of the postal employees I spoke with stated he knows Jeff Sheeder and the week prior Sheeder called the post office asking if a parcel was there for him. At that time, the employee stated there was and Sheeder stated he would be in to pick up the parcel. The employee stated that he physically handed Sheeder the box at the post office. Your affiant asked the employee to describe the box and he/she stated it was a larger box with E-bay tape. Your affiant

asked if he/she could describe Sheeder and he/she stated he had blue eyes with "pencil point" pupils and he was missing a finger on his one hand.

12. When Sheeder returned to the house, I identified myself and showed him the suspect parcel. I asked if he was expecting a parcel and he stated he was not. I asked for consent to open the suspect parcel and Sheeder gave verbal consent as well as filling out IS Form 8193, Consent to Search. Upon opening the parcel approximately 179 xanax pills were found inside a plastic baggy. Sheeder stated he was not expecting them. Sheeder also stated he did not know the sender of the parcel. I then showed Sheeder the box empty box that was found outside his residence. I asked if he ever saw that box before. He stated he did not. I asked if it was not his whose was it, and he stated his friend Caleb was staying at his house and it must be his. I then informed Sheeder that not only was his name on it, but I was able to show that he picked up that parcel from the Everett Post Office. At this time Sheeder stated he did recognize the parcel, that Caleb asked Sheeder to pick it up for him but he did not know the contents. I asked when Caleb asked that and he stated Caleb called him one day asking him to stop by the post office. I asked Sheeder why his name was on the parcel and he could not answer that.

13. At this time, Trooper McCullough asked Sheeder for consent to search the residence. Trooper McCullough explained the Pennsylvania State Police Consent form and advised Sheeder of what was being searched for and stated Sheeder was not in custody, being charged with any crime at this time nor did he have to give consent to search the residence. Sheeder verbally agreed to the search of the residence and then read and signed the form stating he understood. Sheeder then stated there was no money or firearms in the residence, and the only narcotics that would be there was a small amount of marijuana that would be in a plastic jar on his night stand, which he had his medical marijuana card. During this time Sheeder was free to walk around his house and attend to his dog while the search was being conducted.

14. As items were located in the residence, Trooper McCullough took photos of the items in place. On Sheeder's nightstand were three jars, two (2) glass and one (1) plastic, that contained leaf marijuana. Digital scales and indicia, including pay stubs, were found within the night stand. In Sheeder's bedroom closet were mason jars stacked in their cases with a black safe located on top. Sheeder was asked if he had a key to the safe and he stated he did not. Sheeder was told the safe needed to be opened and Sheeder advised "Go ahead and break it open." Upon opening the safe by dropping it on the corner, digital scales, LSD, cocaine, pills, marijuana, psychedelic mushrooms and an unknown substance in a vacuum sealed bag came out of the safe. Also, in the closet was a large amount of marijuana and psychedelic mushrooms in various mason jars. Unused Gelatin caps were also found in the closet. Your affiant was told by Trooper McCullough that the gelatin caps were commonly used in Bedford county to sell cocaine. Sheeder was also in possession of his AT&T cell phone which he advised was in his mother's name. Sheeder attempted to give consent to search the cell phone, however Sheeder was told the phone was going to be seized and a search warrant applied for the phone.

15. At this time, Sheeder stated he did not know any of the aforementioned items were in his house, let alone the closet in his bedroom. It should be noted that aside from all of the narcotics mentioned, personal items of Sheeder's, including clothing and boxes of personal mail and other effects were found in the closet.

16. In the living room of the residence, under a couch, two (2) plastic baggies containing marijuana was located on two metal trays. Sheeder advised the marijuana had to belong to Luzier because he was sleeping on the couch. Sheeder stated Luzier had been living with him for a month or two. Sheeder was asked where Luzier's personal items and clothing was located and Sheeder stated he must have taken everything with him when he left. Sheeder was told Luzier only left with a plastic bag and the clothes he was wearing.

17. Sheeder stated that before he was picked up he spoke with Luzier. Sheeder stated he did not know anything was in the house and Luzier stated to Sheeder the items were his and he would come back and tell investigators if he was called. Using Sheeder's phone, with his permission, Luzier was called twice in a row. Luzier did not answer and his voicemail was not set up.

18. Based on my training and experience, I know the high degree of coordination required to facilitate the receipt, transfer, and delivery of narcotics parcels. Further, I am aware the most frequently used method of communication between individuals involved in drug traffickers is via mobile device.

19. Additionally, traffickers, would be required to know exactly when and where a specific parcel was delivered in order to facilitate its retrieval. In this case, Sheeder knew that a parcel was at the Everett Post Office that was to be delivered to his residence. Based on my training and experience, I know the delivery timeline for parcels can vary, making predicting an exact delivery time and day virtually impossible without utilizing online parcel tracking.

TRAINING AND EXPERIENCE REGARDING DRUG AND FIREARM OFFENSES

20. Based on my training and experience I am aware that the following types of evidence have been recovered from cellular telephone and computer searches, executed in connection with the investigation of drug trafficking:

a. Contact lists, including telephone numbers and names associated with those numbers;

b. Incoming and outgoing call logs;

c. Incoming and outgoing text messages, including draft text messages;

d. Photographs and/or videos;

e. Emails;

f. Online/social media postings; and

g. Banking information.

21. Based on my training and experience, as well as the collective knowledge and experience of other agents and officers associated with this investigation, I am aware that it is common practice for drug traffickers and their co-conspirators to routinely utilize telephones, mobile phones, prepaid phones, calling cards, public telephones, text messaging, counter surveillance, false or fictitious identities, and coded communications, to communicate with their customers, suppliers, couriers, and other conspirators for the purpose of insulating themselves from detection by law enforcement. Moreover, it is not unusual for them to initiate such mobile or prepaid phone service in the name of an associate or family member, or in the name of a fictitious individual. These individuals often require the use of a telephone facility to negotiate times, places, schemes, and manners for importing, possessing, concealing, and distributing controlled substances, and for arranging the disposition of proceeds derived from the sale of controlled substances.

22. Evidence of drug crimes can be found in the electronic media such as cellular telephones, electronic tablets, and personal computers. Such evidence can include internet searches for drug-related paraphernalia, addresses, telephone numbers and contacts, as well as incriminating communications via emails or instant messages. With the advance of technology, the distinction between computers and cellular telephones is quickly becoming less clear. Actions such as internet searching or emailing, in addition to calling and text messaging, can now be performed from many cell phones. In addition, those involved in drug trafficking crimes commonly communicate using multiple cellular telephones and computers. Contemporaneous possession of multiple cellular telephones may be evidence of drug trafficking. Moreover, the particular numbers of, and the particular numbers dialed by, particular cellular telephones may be evidence of drug trafficking,

particularly in a case involving the interception of communications between drug traffickers. Such numbers can confirm the identities of particular speakers and the occurrence of certain events. As with most electronic/digital technology items, communications made from an electronic device, such as a cell phone, are often saved or stored on the device.

23. Your Affiant's awareness of these drug trafficking practices, as well as your Affiant's knowledge of drug use and distribution techniques as set forth in this Affidavit, arise from the following:

a. Your Affiant's involvement in prior drug investigations and searches during her career, as previously described;

b. your Affiant's involvement in interviewing cooperating individuals in prior drug investigations, as well as what other agents and police officers have advised your Affiant of when relating the substance of their similar debriefings and the results of their own drug investigations;

c. discussions with members of the USPIS and/or other federal, state, and local law enforcement officers, both about the facts of this case in particular and about trafficking in general; and

d. other intelligence information provided through law enforcement channels.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

24. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are

designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically

downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in

which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not

scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

25. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

26. Based upon the forgoing, there is probable cause to conclude that, in the Western District of Pennsylvania, SHEEDER has engaged in violations of Title 21, United States Code, Section 846 (drug conspiracy) and Title 21, United States Code, Sections 841(a)(1) (manufacturing, distribution, or possession with the intent to manufacture or distribute a controlled substance).

27. As more fully explained at paragraphs 6-19, there is probable cause to believe that evidence of these crimes will be found upon searching the above Subject Devices.

/s/ *Staci M. Johnson*
Staci M. Johnson
United States Postal Inspector

Sworn and subscribed before me, by telephone
pursuant to Fed.R.Crim.P. 4.1(b)(2)(A),
this 30th day of March 2021.

_____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEM TO BE SEARCHED:

Subject Device – Black and Gray Samsung Phone IMEI: 354266114682650

ATTACHMENT B

PARTICULAR ITEMS TO BE SEIZED

Any and all fruits, contraband, records, evidence and instrumentalities relating to violations violations of Title 21, United States Code, Section 846 (drug conspiracy) and Title 18, United States Code, Sections 1956 and 1957 (money laundering) including:

1. All records on the SUBJECT ELECTRONIC DEVICES described in Attachment A that relate to drug conspiracy in violation of 21 U.S.C. § 846 and/or Title 21, United States Code, Sections 841(a)(1) (manufacturing, distribution, or possession with the intent to manufacture or distribute a controlled substance):

   a. Evidence of communications referring to or relating to illegal narcotics or narcotics trafficking, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

   b. Evidence of communications with suppliers, purchasers, prospective suppliers, or prospective purchasers of illegal narcotics, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

   c. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, or ammunition;

d. Documents, including video and/or audio recordings, in which SHEEDER and/or other individuals discuss or refer to illegal narcotics, drug paraphernalia, firearms, or ammunition;

e. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, ammunition, violence relating to firearms or ammunition;

f. Any and all information revealing the identity of co-conspirators in drug trafficking and/or firearm-related activity;

g. Any and all bank records, transactional records, records of wire transfers, checks, credit card bills, account information, and other financial records;

h. Any and all information suggesting sudden or unexplained wealth of SHEEDER and/or unidentified conspirators;

i. Any and all information identifying the source or entity from whom SHEEDER and/or unidentified conspirators may have secured illegal narcotics, drug paraphernalia, firearms, and/or ammunition;

2. All text messaging, call logs, emails, and/or other records of communication by or involving SHEEDER and/or unidentified conspirators that relate to the planning and operation of drug conspiracy and/or Title 21, United States Code, Sections 841(a)(1) (manufacturing, distribution, or possession with the intent to manufacture or distribute a controlled substance).

3. Evidence of user attribution showing who used, owned, or controlled the SUBJECT ELECTRONIC DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

4. Evidence of software that would allow others to control the SUBJECT ELECTRONIC DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

5. Evidence of the lack of such malicious software.

6. Evidence indicating how and when the SUBJECT ELECTRONIC DEVICE was accessed or used to determine the chronological context of SUBJECT ELECTRONIC DEVICE access, use, and events relating to the crimes under investigation and to the SUBJECT ELECTRONIC DEVICE user.

7. Evidence indicating the SUBJECT ELECTRONIC DEVICE user's state of mind as it relates to the crime under investigation.

8. Evidence of the attachment to the SUBJECT ELECTRONIC DEVICE of other storage devices or similar containers for electronic evidence.

9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT ELECTRONIC DEVICE.

10. Evidence of the times the SUBJECT ELECTRONIC DEVICE were used.

11. Evidence of how the SUBJECT ELECTRONIC DEVICE were used and the purpose of its use including firewall logs, caches, browsing history, cookies, "bookmarked" or "favorite" web pages, temporary Internet directory or "cache," search terms that the user entered into any Internet search engine, records of user-typed web addresses, and other records of or information about the SUBJECT ELECTRONIC DEVICE internet activity.

12. Records of or information about Internet Protocol addresses used by the SUBJECT ELECTRONIC DEVICE.

13. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT ELECTRONIC DEVICE.

14. Documentation and manuals that may be necessary to access the SUBJECT ELECTRONIC DEVICE or to conduct a forensic examination of the SUBJECT ELECTRONIC DEVICE.

15. Contextual information necessary to understand the evidence described in this attachment.

16. All serial numbers or International Mobile Equipment Identity (IMEI) numbers associated with any cellular telephones.

17. Log files, contact information, phone books, voicemails, text messages, draft messages, other stored communication, calendar entries, videos, and photographs related to matters described above.

In searching the SUBJECT ELECTRONIC DEVICE, the federal agents may examine all of the information contained in the SUBJECT ELECTRONIC DEVICE to view their precise contents and determine whether the SUBJECT ELECTRONIC DEVICES and/or information fall within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e.* friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e.* date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents, downloads, status, translations, shared information, GPS, mapping, and other

information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to victims and/or co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data;

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of operating a sophisticated fraud scheme, or other criminal violations;

l. Any handmade form (such as writing);

m. Any mechanical form (such as printing or typing); and

n. Any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, cellular telephones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.